

IN THE CLAIMS

1. (Currently Amended) A method, comprising:
executing a software object;
establishing a security level for said software object, ~~wherein the security level is directly related to said software object;~~
performing a multi-table input/output (I/O) space access using at least one of said security levels, wherein performing the multi-table I/O space access further comprises:
establishing a secondary I/O table;
receiving an I/O space access request based upon executing of said software object;
performing a multi-level table access based upon said I/O space access request using said secondary table and at least one virtual memory table; and
accessing at least a portion an I/O device based upon said multi-level table access;
and
executing a function of said object, wherein executing said function comprising accessing at least a portion of said input/output space.
2. (Original) The method described in claim 1, wherein executing a software object further comprises using a processor to process software code of said software object.

3. (Original) The method described in claim 1, wherein establishing a security level for said software object further comprises assigning a security level relating to an I/O space access of at least a portion of a memory.

4. (Canceled)

5. (Currently Amended) The method described in claim [[4]]1, wherein establishing a secondary table further comprises:

dividing an I/O space into a plurality of segments;

determining at least one of said segment to omit from said secondary I/O table and at least one un-omitted segment;

assigning a default security level to said omitted segment;

assigning a security level to said un-omitted segment; and

correlate at least one assigned segment with an I/O space location.

6. (Currently Amended) The method described in claim [[4]]1, wherein performing a multi-level table access based upon said I/O space access request further comprises:

determining at least one security level that corresponds to a segment in said secondary I/O table;

verifying a match between an execution security level to a security level associated with a segment being accessed in response to an execution of said object;

determining an I/O space addresses based upon said secondary table in response to a match between said execution security level and said security level associated with said segment being accessed; and
locating an I/O device corresponding to said I/O space address.

7. (Original) The method described in claim 6, wherein determining at least one security level that corresponds to a segment in said secondary I/O table comprises:

determining a physical I/O device address from said secondary I/O table;
determining a segment being executed based upon said physical I/O device address; and
defining a current security level based upon said determining of said segment being executed.

8. (Previously Presented) A method, comprising:

executing a software object;
establishing a security level for said software object;
establishing a secondary input/output (I/O) table;
receiving an I/O space access request based upon executing of said software object;
determining at least one security level that corresponds to a segment in said secondary I/O table;
verifying a match between an execution security level to a security level associated with a segment being accessed in response to an execution of said software object;

determining an I/O space address based upon said secondary I/O table in response to a match between said execution security level and said security level associated with said segment being accessed;

locating a physical I/O device location corresponding to said I/O space address; and

accessing a portion of an I/O device based upon locating said physical memory location.

9. (Original) The method described in claim 8, wherein executing a software object further comprises using a processor to process software code of said software object.

10. (Original) The method described in claim 8, wherein establishing a security level for said software object further comprises assigning a security level relating to an I/O space access of at least a portion of an I/O device.

11. (Original) The method described in claim 8, wherein determining at least one security level that corresponds to a segment in said secondary I/O table comprises:

determining a physical I/O device address from said I/O space table;

determining a segment being executed based upon said physical I/O device address; and

defining a current security level based upon said determining of said segment being executed.

12. (Currently Amended) An apparatus, comprising:

means for executing a software object;

means for establishing a security level for said software object, ~~wherein the security level~~
~~is directly related to said software object;~~

means for performing a multi-table input/output (I/O) space access using at least one of
said security levels, wherein means for performing the multi-table I/O space
access further comprises:

means for establishing a secondary I/O table;

means for receiving an I/O space access request based upon executing of said
software object;

means for performing a multi-level table access based upon said I/O space access
request using said secondary table and at least one virtual memory table;

and

means for accessing at least a portion an I/O device based upon said multi-level
table access; and

means for executing a function of said object, wherein means for executing said function
comprising means for accessing at least a portion of said input/output space.

13. (Currently Amended) An apparatus, comprising:

a processor coupled to a bus;

means for coupling at least one software object to said processor;

an input/output (I/O) device; and

an (I/O) access interface coupled to said bus and said memory unit, said memory access
interface to provide said processor a multi-level table I/O space access of at least
a portion of said memory unit based upon at least one security level, in response

to said processor executing said software object, ~~wherein the security level is directly related to said software object~~ wherein said I/O space access interface comprises an I/O space access table coupled with a secondary I/O table, said memory access interface to provide a virtual memory addressing scheme to access at least one portion of said I/O device based upon a security level.

14. (Original) The apparatus of claim 13, wherein said processor comprises at least one microprocessor.

15. (Canceled)

16. (Original) The apparatus of claim 13, wherein said I/O device comprises a memory that comprises at least one of a magnetic tape memory, a flash memory, a random access memory, and a memory residing on a semiconductor chip.

17. (Original) A computer readable program storage device encoded with instructions that, when executed by a computer, performs a method, comprising:

executing a software object;

establishing a security level for said software object;

establishing a secondary input/output (I/O) table;

receiving an I/O space access request based upon executing of said software object;

determining at least one security level that corresponds to a segment in said secondary I/O table;

verifying a match between an execution security level to a security level associated with a segment being accessed in response to an execution of said software object; determining an I/O space addresses based upon said secondary I/O table in response to a match between said execution security level and said security level associated with said segment being accessed; locating a physical I/O device location corresponding to said I/O space address; and accessing a portion of an I/O device based upon locating said physical memory location.

18. (Original) The computer readable program storage device encoded with instructions that, when executed by a computer, performs the method described in claim 17, wherein executing a software object further comprises using a processor to process software code of said software object.

19. (Original) The computer readable program storage device encoded with instructions that, when executed by a computer, performs the method described in claim 17, wherein establishing a security level for said software object further comprises assigning a security level relating to an I/O space access of at least a portion of an I/O device.

20. (Original) The computer readable program storage device encoded with instructions that, when executed by a computer, performs the method described in claim 17, wherein determining at least one security level that corresponds to a segment in said secondary I/O table comprises:

determining a physical I/O device address from said I/O space table;

determining a segment being executed based upon said physical I/O device address; and
defining a current security level based upon said determining of said segment being
executed.